ANOMALI

MITRE ATT&CK and Anomali

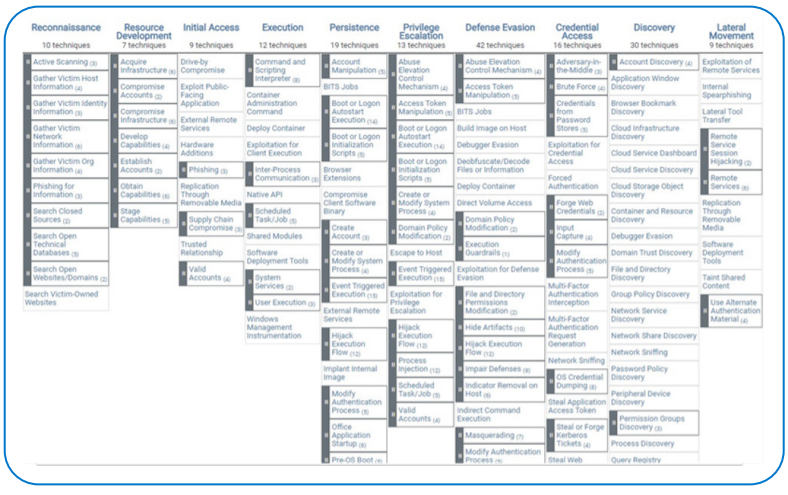
Security operations teams spend too much time manually combing through alerts to identify threats. Unfortunately, malicious activity can slip through unrecognized, despite best efforts. The harsh reality is that attackers are penetrating most environments without being detected.

Organizations need to look beyond IOCs to enable more effective threat detection and response to improve their security posture. The MITRE ATT&CK framework adds significant value for security teams as it focuses on the attackers' adversarial tactics, techniques, and procedures.

Anomali has integrated the ATT&CK framework to help security teams visualize an attacker's motivations to better understand their actions and quickly defend against security risks.

By operationalizing MITRE ATT&CK, security analysts can answer critical questions, including:

- Are my security tools working as expected?
- How can I assess and reduce risk?
- Am I optimizing the value from my security controls expenditures?
- Are we protected against an imminent threat?



KEY USE CASES

ELEVATE STAFF PRODUCTIVITY

Empower security professionals to better identify and disrupt malicious activity

OPERATIONALIZE INSIGHTS

Discover adversarial techniques on web-based content and convert it to actionable insights about your threat landscape

RECOGNIZE THREATS ON THE GROUND

Understand adversarial techniques and how they are being leveraged against your environment

VISUALIZE THREAT MODELS

Build visual representations of techniques employed by threat actors and malware

Key Benefits:

Recognizing the power of MITRE ATT&CK, Anomali integrated ATT&CK into the Anomali solution suite to enable analysts to:

- Empower security professionals to better identify and disrupt malicious activity
- Discover adversarial techniques from raw data and convert it to actionable insights about your threat landscape
- Understand adversarial techniques and how they are leveraged against your environment
- Build visual representations of techniques employed by threat actors and malware

THREATSTREAM

Transform threat data into relevant, actionable intelligence to speed detection and increase analyst productivity.

- PROFILE YOUR ADVERSARIES - Quickly identify the Attack Patterns and TTPs used by threats targeting your organization.
- SHARE THREATS ACROSS TRUSTED COMMUNITIES - Securely collaborate with internal colleagues and peers at similar organizations to speed threat identification and get advice to help manage threats.
- TRACK YOUR SECURITY COVERAGE - Prioritize prevention and remediation by highlighting security gaps in the MITRE ATT&CK visualization.
- CONNECT INVESTIGATIONS TO OPERATIONAL INTELLIGENCE - Visualize MITRE TTT&CK patterns and impact as you build out your investigation.

MATCH

Detect and respond in real-time by automatically correlating ALL security telemetry against active threats.

- PINPOINT RELEVANT THREATS - Learn in seconds if a threat indicator is present in your historical event logs, asset data, vulnerability scan data, and threat intelligence going back at least five years.
- ELEVATE STRATEGIC INTELLIGENCE - View alerts enriched with comprehensive threat intelligence context, MITRE ATT&CK Framework IDs, asset criticality, and risk scores.
- ACCELERATE THREAT HUNTING - Proactively identify threats in your environment based on MITRE ATT&CK TTPs, actors, campaigns, threat bulletins, and vulnerabilities.
- ANTICIPATE THE NEXT ATTACK - Gain relevant visibility through continuous attacker monitoring to uncover threats and anticpate an attacker's next move.

LENS

Surface threat insights from raw data to automate and operationalize threat intelligence research.

- INGEST UPDATED DATA ON IOCS - Scan phishing emails, malicious email addresses, URLs, and hashes from a source portal or website, then export the data into ThreatStream automatically.
- OPERATIONALIZE MITRE ATT&CK - Associate scanned and imported techniques with MITRE ATT&CK IDs, then export to an investigation with one click.
- DETERMINE IMPACT QUICKLY - Automatically determine whether a scanned threat indicator or TTP has been seen in your environment.
- INFORM YOUR ORGANIZATION - Create professional-quality reports to inform management and threat detection, response, and remediation efforts.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI